

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

Civil No: 14 -

DISH NETWORK L.L.C, ECHOSTAR
TECHNOLOGIES L.L.C., and NAGRASTAR
LLC

Plaintiffs

v.

Edgardo Carrasquillo Reyes, a/k/a "Edgardo
Carrasquillo", "Ed Reyes", "Frank Reyes",
"BluebirdPR" and "Bluebird" d/b/a Generation
IKS, www.caribbeansystems.galeon.com
and JOHN DOES 1-3

Defendant

DECLARATION OF GREGORY DUVAL IN
SUPPORT OF PLAINTIFFS' *EX PARTE*
MOTIONS FOR TEMPORARY RESTRAINING
ORDER, CIVIL SEIZURE/ IMPOUNDMENT
ORDER, ORDER TO SHOW CAUSE, ORDER
TEMPORARILY SEALING CASE, ORDER
FOR ASSET FREEZE, AND ORDER FOR
ACCOUNTING AND SUMMARIZATION OF
OTHER DECLARATIONS

DECLARATION OF GREGORY DUVAL

1. My name is Gregory Duval.
2. I am making this declaration in support of the Plaintiffs' Ex Parte Motions for Temporary Restraining Order, Civil Seizure/Impoundment Order, Order to Show Cause, Order Temporarily Sealing Case, Order for Asset freeze and Order for Accounting.
3. The facts set forth in this declaration are within my personal knowledge, true and correct, and I would testify to them under oath if called upon to do so.

Personal Background

4. I am currently employed as Chief Operating Officer with Plaintiff NagraStar LLC ("NagraStar"), the supplier of proprietary encryption technology utilized by Plaintiffs DISH Network L.L.C., and EchoStar Technologies L.L.C.

5. I became employed by NagraStar in 2005, bringing several years of experience in the field of conditional access and security solutions for satellite television systems. Prior to that time, I was employed by NagraStar's co-founder and part owner, NagraVision S.A., as the head of engineering and conditional access system architect. In that capacity, I acquired a comprehensive understanding of the security system or conditional access system used by DISH Network.

6. At NagraStar, I currently supervise several internal departments, including system security, system support, system testing, architecture, and research and development. My primary responsibilities with NagraStar are the development and deployment of the conditional access system or security system protecting DISH Network satellite television programming and leading all anti-piracy operations pertaining to that security system.

Plaintiffs DISH Network, EchoStar Technologies, and NagraStar

7. DISH Network is a multi-channel video provider that delivers video, audio, and data to approximately 14 million authorized subscribers in the United States, Puerto Rico, and the U.S. Virgin Islands using direct-to-home satellite services via a direct broadcast satellite system.

8. DISH Network uses high-powered satellites to broadcast, among other things, movies, sports, and general entertainment services to consumers who have been authorized to receive such services after payment of a subscription fee, or in the case of a pay-per-view movie or event the purchase price.

9. DISH Network contracts for and purchases the distribution rights for most of the programming broadcast on the DISH Network platform from providers such as network affiliates, motion picture distributors, pay and specialty broadcasters, cable networks, sports leagues, and other holders of programming rights.

10. The works broadcast by DISH Network are copyright protected. DISH Network has the authority of the copyright holders to protect the works from unauthorized access, reception, and viewing.

11. DISH Network programming is digitized, compressed, and scrambled or encrypted prior to being transmitted to multiple satellites located in geo-synchronous orbit above Earth. The satellites, which have relatively fixed footprints covering the United States and parts of Canada, Mexico, and the Caribbean, relay the encrypted signal back to Earth where it can be received by DISH Network subscribers that have the necessary equipment.

12. A DISH Network satellite television system consists of a compatible dish antenna, receiver, smart card which in some instances is internalized in the receiver, television, and cabling to connect the components. EchoStar Technologies L.L.C. provides receivers, dish antenna, and other digital equipment for the DISH Network system. Smart cards and other proprietary security technologies that form a conditional access system are supplied by NagraStar LLC.

13. Each EchoStar Technologies receiver and NagraStar smart card is assigned a unique serial number that is used by DISH Network when activating the equipment and to ensure the equipment only decrypts programming the customer is authorized to receive as part of his subscription package and pay-per-view purchases.

14. The DISH Network security system performs two interrelated functions in the ordinary course of its operation: first, subscriber rights management, which allows DISH Network to “turn on” and “turn off” programming a customer has ordered, cancelled, or changed; and second, protection of control words that are contained within and that descramble DISH Network’s satellite signal, which prevents unauthorized access, reception, and viewing of DISH Network programming.

15. An integral part of DISH Network's security system is a smart card having a secure embedded microprocessor that functions as a security computer. The microprocessor contains a ROM segment of memory that provides instructions and commands to the smart card in the everyday operation of the DISH Network security system. The ROM segment reads from data stored within the microprocessor's EEPROM to perform its calculation and operation functions. The EEPROM segment also stores, among other things, a special kind of data called decryption keys.

16. The EchoStar Technologies receiver processes an incoming DISH Network satellite signal by locating an encrypted part of the transmission known as the entitlement control message and forwards it to the smart card. Provided that the subscriber is tuned to a channel he is authorized to watch, the smart card uses its decryption keys to unlock the message, uncovering a control word. The control word is transmitted back to the receiver in order to decrypt the DISH Network satellite signal.

17. Together, the EchoStar Technologies receiver and NagraStar smart card convert DISH Network's encrypted satellite signal into viewable programming that can be displayed on the attached television of an authorized DISH Network subscriber.

Piracy of DISH Network Programming

18. Several years ago pirates developed a method to circumvent the DISH Network security system and intercept DISH Network's satellite broadcasts using so-called "free-to-air" or "FTA" receivers ("unauthorized receivers"). Initially, this method of piracy was accomplished by loading software that contains the proprietary data and keys to DISH Network's security system ("piracy software") onto circuit chips in the unauthorized receiver, so as to mimic a legitimate NagraStar smart card.

19. Piracy software is made available for free on various internet websites, and once downloaded, is transferred to an unauthorized receiver through a connection to a home computer or thumb drive. The process of loading piracy software is referred to as “flashing” the receiver and can be completed by even a layperson in a matter of minutes.

20. The downside of the foregoing method of signal theft is that piracy software must be regularly updated to account for and overcome changes in DISH Network’s security system, such as electronic countermeasures transmitted in the satellite stream. These countermeasures have many effects, one being to change the decryption keys required to access proprietary DISH Network control words. As a result, a new form of satellite piracy emerged and goes by several names including “control word sharing,” “Internet key sharing,” or more simply “IKS.”

21. With IKS, once piracy software is loaded onto the unauthorized receiver, the end user connects the receiver to the internet via the receiver’s built-in Ethernet port or via an add-on dongle. The internet connection serves two piracy-related purposes: first, it automatically updates piracy software on the receiver; and second, the internet connection contacts a computer server which in turn provides the DISH Network control words needed to decrypt or descramble the encrypted DISH Network television programming.

22. The computer server, called an “IKS server,” has multiple, subscribed NagraStar smart cards connected to it, and thus, the ability to provide control words. Access to an IKS server typically requires a valid access code, which can be purchased or obtained through a subscription service. Once access has been obtained, control words are sent from the IKS server over the internet to an unauthorized receiver, where they are used to decrypt DISH Network’s signal and allow for the viewing of DISH Network programming without paying a subscription fee. Alternatively, control words can also be sent from the IKS server to another IKS server over the

internet, which will then send the control words to an unauthorized receiver to decrypt DISH Network's signal and allow for the viewing of DISH Network programming without paying a subscription fee.

23. Because IKS is based on the trafficking of control words illegally obtained from legitimate DISH Network receiving equipment, this method of satellite piracy remains effective even after DISH Network's transition to "Nagra 3" or "N3," a third generation security technology recently introduced by NagraStar.


Satellite Piracy Causes Substantial, Irreparable Harm to Plaintiffs

24. DISH Network, EchoStar Technologies, and NagraStar invest millions of dollars each year in the security measures that protect DISH Network programming from unauthorized viewing. The selling and distribution of IKS services and devices, including Fire Share Load Balance (FSLB), RQ Card Server Program, and Fireshare EMM feeder (FSEF) software programs, that circumvent these security measures, however, eradicates the investment in the technology and undermines the values that the technological measures are meant to preserve, chief among them the ability to control access to the copyrighted programming broadcast on the DISH Network platform, which is lost when unauthorized circumvention and decryption devices are used by satellite television pirates. When an end user subscribes to an IKS subscription service or obtains IKS server access codes, piracy software, and an unauthorized receiver and uses them to access an IKS server, the end user has the ability to circumvent DISH Network's security system and receive and decrypt DISH Network programming without authorization and without payment of a subscription fee to DISH Network, resulting in a loss of customers and market share.

25. Equally serious is the damage to the business reputation and goodwill of DISH Network, EchoStar Technologies, and NagraStar. Their reputations are built on and depend on the delivery of secured content. Piracy harms those reputations and interferes with the contractual and prospective business relationships of DISH Network, EchoStar Technologies, and NagraStar, including relations with programming providers and customers for set-top boxes and security system solutions. Calculating the business reputational damage due to this impact is inherently difficult, if not impossible.

26. Satellite piracy directly and negatively impacts the revenues earned by DISH Network, EchoStar Technologies, and NagraStar. The injury to DISH Network includes lost programming revenues and profits that would customarily be paid by a legitimate DISH Network subscriber. DISH Network's average monthly revenue per authorized subscriber is approximately \$70 each month. An untold number of individuals who use IKS services, IKS server access codes, piracy software, and unauthorized receivers to connect to an IKS server to receive unauthorized control words, however, have unlimited access to view DISH Network programming, including premium and pay-per-view channels, the value of which far exceeds that built in the average subscriber calculation. Similarly, piracy deprives NagraStar and EchoStar Technologies of revenues and profits that would ordinarily be gained from the sale of receivers, smart cards, and other technology to legitimate subscribers.

I affirm this 4 day of June, 2014 under penalty of perjury pursuant to the laws of the United States that the foregoing is true and correct.



Gregory Duval